NSCS Information Security Standard 2: Responsibilities, Enforcement, and Exceptions

NSCS information security responsibilities are distributed among the following offices and personnel.

2.1 NSCS Board of Trustees

Approves the NSCS Information Security Board Policy and promotes the consistent and full implementation of the Policy in support of the NSCS's vision and mission.

2.2 Vice Chancellor for Facilities & Information Technology and System Office Information Security Officer (SOISO)

Oversees the development and maintenance of Information Security Policy and associated Standards, facilitates the NSCS Information Security Board Policy approval process, and provides leadership for the continued development of a robust and secure information technology environment throughout the NSCS. Coordinates security initiatives among the NSCS System Office and Colleges. Periodically reviews external security frameworks (NIST, PCI, FERPA, etc.) and updates NSCS Standards as needed, no less than every two (2) years.

2.3 College Chief Information Officers (CIO's) and Chief Information Security Officers (CISO's)

The CIO's offices provide leadership for the continued development of a robust and secure information technology environment within their respective Colleges. Within NSCS, the role of CISO is assigned by the respective President. The CISO enables the College to conduct its business in a secure manner while achieving regulatory compliance. Responsibilities include oversight of the College's Information Security Program.

2.4 Information Technology Staff

Provides and supports an infrastructure that meets the needs of its respective academic and administrative community in compliance with NSCS Policy and the College's Information Security Program.

2.5 Data Steward

Classifies the data that they manage in compliance with NSCS Information Security Standard 4.1 Data Classification and ensure that the CISO is informed of the data classification.

2.6 Users

Employees, students, contractors and guests required to adhere to the requirements of NSCS Information Security Policy and Standards and any specific College procedures.

2.7 Policy Compliance

The CIO/CISO at each College is responsible for ensuring compliance with NSCS Information Security Policy and associated Standards at his/her assigned College. The Vice Chancellor for Facilities & Information Technology/SOISO is responsible for ensuring compliance at the System Office and NSCS level.

2.8 Policy Exceptions

The Vice Chancellor for Facilities & Information Technology will coordinate exception requests to NSCS Information Security Standards at the Systems Office level and may consult with the College Chief Information Officers/Chief Information Security Officers (CIOs/CISOs) and other authorities as deemed appropriate for resolution of the exception request. The CIO/CISO will coordinate exception requests at his/her assigned College and will contact the respective data steward and other authorities as deemed appropriate for consideration and resolution of the exception request. The required data elements of an Information Security Standards Exception Form are noted below. Approved exception requests shall be re-evaluated on an annual basis to determine if the exception is still needed or if the risk associated with the exception remains acceptable, and the decision will be electronically documented to the original requestor.

2.9 Exception Form Required Data Elements

- Standard impacted
- Business Process reason for exception
- Proposed resolution
- Requestor
- Workflow details (sign-off, etc.)
- Request date

Revision History

April/14/2019: Initial submission by PCSS
May/8/2019: Initial review by SOISO/CISOs
July/8/2019: Second review by SOISO/CISOs
July/26/2019: Third review by SOISO
Oct/1/2019: Fourth review by SOISO